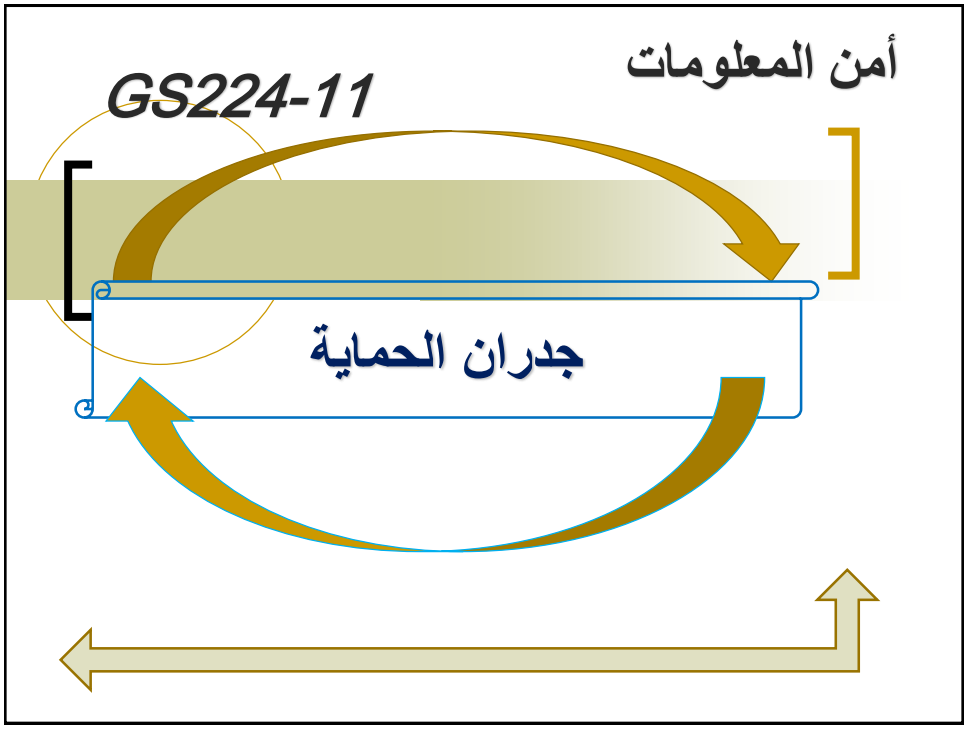


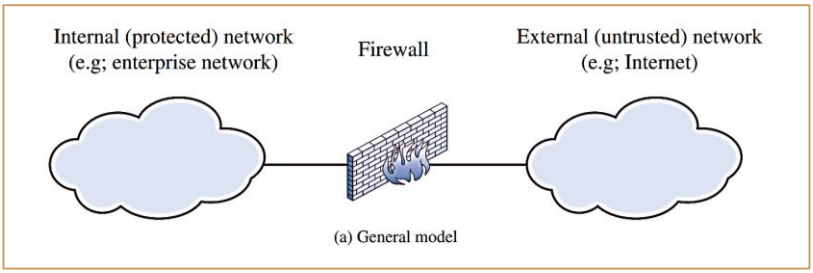
نظام جدار الحماية (Firewall)

جدران الحماية هي وسيلة فعالة لحماية نظام محلي أو شبكة من الأنظمة من التهديدات الأمنية للشبكات وتتيح في نفس الوقت الوصول إلى العالم الخارجي عبر شبكات الإنترنت.

لم يعد الاتصال بالإنترنت اختياريًا للمؤسسات ، فالمعلومات والخدمات المتاحة على الانترنت ضرورية للمؤسسة. علاوة على ذلك ، يحتاجها المستخدمون داخل المؤسسة، وإذا لم يتم توفير ذلك عبر شبكة المحلية الخاصة بالمؤسسة ، فسيستخدمون إمكانية الاتصال الهاتفي من حواسيبهم الخاصة إلى مزود خدمة الإنترنت (ISP) . وكما يوفر الوصول إلى الإنترنت فوائد للمؤسسة ، فإنه يمكّن العالم الخارجي من الوصول إلى الشبكة المحلية للمؤسسة والتفاعل معها ، وهذا يخلق تهديدا للمنظمة.

ومن الممكن تجهيز كل محطة عمل وخادم في محيط الشبكة بميزات أمان قوية ، مثل الحماية من التسلل و الاختراق ، ولكن هذا ليس نهجًا عمليًا. البديل ، والمقبول بشكل متزايد هو **جدار الحماية الذي يتم وضعه بين محيط شبكة المحلية والإنترنت لإنشاء ارتباط متحكم به وإقامة جدار أمن على محيط الشبكة. الهدف من هذا هو حماية محيط الشبكة من الهجمات المعتمدة إلى الإنترنت وتوفير عنق مرور واحد حيث يمكن فرض الأمن والتدقيق، بحيث ان كافة الرسائل القادمة من الانترنت او المتجهة اليها تمر بجدار الحماية، ومن ثم يكون بمقدور جدار الحماية فحص هذه الرسائل سواء كانت بريدا الكترونيا و ملفات متبادلة او محاولات دخول للشبكة عن بعد او أي نوع من الاتصال وبناء على نتيجة الفحص يقوم بالتصريح لهت بالمرور اذا كانت تتفق مع السياسة الأمنية للمؤسسة.**

نظام جدار الحماية (Firewall)



(a) General model

سياسة الوصول لجدار الحماية

يعد تحديد سياسة وصول مناسبة أحد المكونات الحاسمة في تخطيط جدار الحماية وتنفيذه. يجب تطوير هذه السياسة عبر تقييم المخاطر و سياسة أمن المعلومات في المؤسسة. يجب تطوير هذه السياسة من خلال المواصفات الموسعة لأنواع حركة المرور التي تحتاج المؤسسة إلى دعمها. من ثم يتم تنقيحها لتحديد تفصيل عناصر التصفية ، والتي يمكن بعد ذلك تنفيذها ضمن عمارة جدار حماية مناسب.
يتكون جدار الحماية في المعتاد من بعض الأجهزة مثل الموجهات و الحاسبات بالإضافة لبعض البرمجيات التي تتولى تنفيذ السياسة الأمنية، لذلك يتم تهيئة جدار الحماية لتنفيذ هذه السياسة.

الأهداف المرجوة في تصميم جدار الحماية:

1) يجب أن تمر جميع حركات المرور من الداخل إلى الخارج ، والعكس بالعكس ، عبر جدار الحماية. يتم تحقيق ذلك عن طريق حظر كل الوصول إلى الشبكة المحلية ما عدا التي تمر عبر جدار الحماية.
2) يسمح فقط بالمرور المرخص به ، كما هو محدد في سياسة الأمن المحلية. يتم استخدام أنواع مختلفة من جدران الحماية ، والتي تنفذ أنواعًا مختلفة من سياسات الأمان.
3) جدار الحماية نفسه محصن ضد الاختراق. هذا يعني استخدام نظام منيع مع نظام تشغيل آمن. أنظمة الحاسوب الموثوقة المناسبة لاستضافة جدران الحماية وغالبًا ما تكون مطلوبة في التطبيقات الحكومية.

سياسة الوصول لجدار الحماية

هناك مجموعة من الخصائص التي يمكن لسياسة الوصول لجدار الحماية استخدامها لتصفية حركة المرور ، بما في ذلك:

1) نطاق عناوين (IP) وقيم البروتوكولات: يتحكم في الوصول استنادًا إلى عناوين المصدر أو الوجهة وأرقام المنافذ واتجاه التدفق الداخل أو الخارج والخصائص الأخرى لطبقة النقل والشبكة. يتم استخدام هذا النوع من التصفية بواسطة مرشح الحزمة وجدران حماية المعتمدة على تفتيش الحالة. ويتم استخدامه عادةً لتقييد الوصول إلى خدمات معينة.
2) بروتوكولات التطبيقات: يتحكم في الوصول على أساس بيانات البروتوكول الذى يستخدمه التطبيق المصرح به. يتم استخدام هذا النوع من التصفية بواسطة بوابة على مستوى التطبيق تقوم بترحيل ومراقبة تبادل المعلومات لبروتوكولات تطبيقات معينة ، على سبيل المثال ، التحقق من بريد (SMTP) الإلكتروني بحثًا عن البريد المزعج ، أو طلبات ويب (HTTP) للمواقع المصرح بها فقط.
3) هوية المستخدم: يتحكم في الوصول استنادًا إلى هوية المستخدمين ، عادةً للمستخدمين الداخليين الذين يعرّفون أنفسهم باستخدام شكل من أشكال تقنيات المصادقة الآمنة ، مثل (IPSec).
4) نشاط الشبكة: يتحكم في الوصول بناءً على اعتبارات معينة مثل الوقت أو الطلب ، على سبيل المثال ، فقط في ساعات العمل ؛ معدل الطلبات ، على سبيل المثال ، للكشف عن محاولات المسح ؛ أو أنماط نشاطات أخرى.

قدرات جدار الحماية

تقع الامكانات التالية ضمن نطاق قدرات جدار الحماية:

1) يحدد جدار الحماية نقطة اختناق واحدة تُبقي المستخدمين غير المصرح لهم خارج الشبكة المحمية ، ويمنع الخدمات التي يُحتمل أن تكون معرضة للخطر من دخول الشبكة أو مغادرتها ، ويوفر الحماية من أنواع مختلفة من هجمات انتحال عناوين (IP) و المسارات. يؤدي تركيز الإجراءات الأمنية في نقطة واحدة إلى تبسيط إدارة الأمن وذلك افضل من توزيعها بين نقاط مختلفة وأجهزة مختلفة.
2) يوفر جدار الحماية موقعًا لمراقبة الأحداث المتعلقة بالأمن وفرضها. فجدار الحماية اشبه بشرطي المرور فيما يخص استفادة المستخدمين من خدمات الانترنت فيسمح بهذه الخدمة او يمنعها تبعا للسياسة الأمنية للمؤسسة. كذلك تسجيل وقائع الاستخدام بدقة طالما ان كل الرسائل والاوامر تمر به عند خروجها الى الانترنت او قدومها منها.
3) يعد جدار الحماية نظامًا أساسيًا مناسبًا للعديد من وظائف الإنترنت الغير مؤمنة. يتضمن ذلك برتوكول مترجم عنوان الشبكة (NAT) ، ووظيفة إدارة الشبكة التي تقوم بتدقيق استخدام الإنترنت أو تسجيل الوقائع. كما يمكن لجدار الحماية أن يعمل كمنصة لبرتوكول (IPSec) لإنجاز الشبكات الافتراضية الخاصة.
4) الحد من درجة تعرض الشبكة للأخطار، وربما كانت هذه هي اهم الفوائد لحماية الشبكة الداخلية من اخطار الانترنت، او أحيانا لحماية بعض اقسام الشبكة الداخلية من بعضها الاخر.

قيود جدار الحماية

للجدران النارية حدودها ، بما في ذلك ما يلي:

1) قد لا يوفر جدار الحماية الكاملة من التهديدات الداخلية ، مثل موظف ساخط أو موظف يتعاون عن غير قصد مع مهاجم خارجي. فموقع جدار الحماية هو على حدود الشبكة ولا يستطيع ان يفعل الكثير لمهاجم من الداخل يريد سرقة المعلومات من احد الأجهزة الداخلية، او تخريب الأجهزة او البرامج او تعديلها، لأنها ستتم بعيدا عن (أعين) جدار الحماية.
2) لا يمكن لجدار الحماية من الهجمات التي تتم من الاتصالات التي لا تمر عبر جدار الحماية ، فاذا سمحت مؤسسة بالارتباط بالأنترنت من خلال الاتصال الهاتفي (مودم) مركب في احد حواسيب المستخدمين دون المرور بجدار الحماية فلا يستطيع جدار الحماية فعل شيء.
3) الاخطار الجديدة تمام و التي لم يصمم جدار الحماية مسبقا للحماية منها، فجدار الحماية لا يستطيع التأقلم (فوريا) لمواجهة أي سيناريو لإحداث يفاجأ به. لذلك يجب تحديث تهيئة جدران الحماية باستمرار لمواكبة ما يتم اكتشافه من أفكار جديدة.
4) الحماية التامة من الفيروسات، فبرغم من قدرته على حجب الكثير من الفيروسات، الا ان ذلك لا يتم بصورة كاملة تكفى للاستغناء عن اقتناء برنامج الحماية من الفيروسات.
5) التهيئة الذاتية؛ فجدار الحماية يحتاج لمن يقوم بتهيئته لا كل موقع يختلف عن الموقع الاخر في طبيعته و سياسته الأمنية. ولذلك لا يمكن ان تشترى جدار حماية (جاهزا) يتم تركيبه دون بذل جهد في تهيئته و تدريبه فضلا عن اختباره من البداية ، و الا كان الأثر عكسيا و اعطانا جدار الحماية إحساسا زائفا بالأمان.

جدران الحماية : مصفاة الحزم

مصفاة الحزم: يطبق مجموعة من القواعد (الفحص) على كل حزمة (IP) واردة وصادرة ثم يعيد توجيه الحزمة أو يتجاهلها. يتم تهيئة جدار الحماية عادةً لتصفية الحزم التي تذهب في كلا الاتجاهين (من وإلى الشبكة الداخلية). تستند قواعد التصفية إلى البيانات الموجودة في الحزمة او بعض الحقول في مقدمة الحزمة، ومن بين الحقول التي يتم فحصها بواسطة هذا النوع من جدران الحماية :

- مصدر الحزمة (المرسل) و وجهة الوصول (المستقبل).
- المنفذ المستخدم (Port).
- نوع البرتوكول المستخدم (TCP, UDP, …).
- نوع الخدمة المؤدة (FTP, Telnet, DNS, RIP, …).

ويتم تركيب "مصفاة الحزم" عادة في احدى صورتين: اما كموجه حاجب (Screening router) او كحاسب محصن (Bastion host) وكلاهما ببطاقات شبكة متعددة. الموجه الحاجب هو عبارة عن حاسب مخصص للتحكم في مرور الحزم بين اقسام الشبكة، او بينها و بين شبكة الانترنت، بينما الحاسب المحصن هو عبارة عن حاسب عادى تمت تقويته (تحصينه) عن طريق حذف أي برامج غير ضرورية او أي برامج قد تسبب اضعافا لأمن الشبكة.

جدران الحماية : مصفاة الحزم

عادةً ما يتم إعداد عامل تصفية الحزمة كقائمة من القواعد بناءً على التطابقات مع الحقول الموجودة في الحزمة. إذا كان هناك تطابق مع إحدى القواعد ، يتم استدعاء هذه القاعدة لتحديد ما إذا كان سيتم إعادة توجيه الحزمة أو تجاهلها. إذا لم يكن هناك تطابق مع أي قاعدة ، فسيتم اتخاذ إجراء افتراضي. هناك سياستان افتراضيتان ممكنتان:

- الافتراض = حظر: محظور ما لم يُسمح بذلك صراحة : أكثر تحفظًا ومحكم وواضح للمستخدمين.
- الافتراض = تمرير: مسموح ما لم يحظر صراحة : أسهل في الإدارة / الاستخدام ولكن أقل أمانًا

سياسة التجاهل الافتراضية أكثر تحفظًا. في البداية ، يتم حظر كل شيء ، ويجب إضافة الخدمات على أساس كل حالة على حدة. هذه السياسة أكثر وضوحًا للمستخدمين ، الذين من المرجح أن يروا جدار الحماية على أنه عائق. تزيد سياسة إعادة التوجيه الافتراضية من سهولة الاستخدام للمستخدمين النهائيين ولكنها توفر أمانًا أقل ؛ يجب على مسؤول الأمن ، في الاساس ، الرد على كل تهديد أمني جديد كما هو معروف.

يمكن تقسيم هذا النوع من جدران الحماية الى نوعين فرعيين هما: مصفاة الحزم الاستاتيكية (Static packet filter)، ومصفاة الحزم الديناميكية (Dynamic packet filter).

مصفاة الحزم : مصفاة الحزم الاستاتيكية

يتحكم هذا النوع في تمرير الحزم عن طريق استخدام المعلومات الموجودة في مقدمة الحزمة (Packet header)، وذلك بمقارنتها مع قائمة التحكم في الاستخدام (Access Control List) المخزنة في المصفاة ومن ثم يتخذ قرار التمرير من عدمه. ولاتخاذ القرار الصحيح يتم فحص عنوان الجهة المرسلة، وعنوان الجهة المستقبلة، ورقم منفذ الخدمة، وحقل العلامات (TCP flags) الذى يبين طبيعة الحزمة. وهذا الحقل يحتوى على مجموعة من العلامات (flags) التي تكون نشطة (1 =) او خاملة (0 =). ويلعب هذا الحقل (حقل العلامات) دورا هاما في مساعدة مصفاة الحزم الاستاتيكية على أداء مهمتها، لأنه من غير المعتاد ان نطلب من جدار الحماية منع كل البريد الوارد من موقع معين، بل لابد ان تكون هناك شروط لهذا المنع، ومعظم هذه الشروط يمكن معالجتها بفحص هذا الحقل. فقد تكون السياسة الأمنية هي مثلا: يسمح للمستخدمين باستخدام شبكة الانترنت و لكن تمنع أي رسائل واردة من شبكة الانترنت. ومن ثم لابد للمصفاة عند استقبالها للرسائل الواردة من الانترنت ان تتأكد أولا ان الرسالة ليست ردا (جواب)، او استجابة لطلب مرسل من الشبكة للأنترنت. فتقوم المصفاة بمنع كل الرسائل الواردة، ماعدا تلك الواردة كاستجابة. وتستطيع المصفاة معرفة نوع الرسالة الواردة، هل استجابة ام لا، عن طريق اختبار حقل العلامات (TCP flags) و التأكد من يحتوى على العلامة (ACK) في الحالة النشطة (ACK=1)، أي ان هذه الرسالة هي استجابة (جواب) لطلب بيانات من الحاسب قد سبق ارساله.

ولذلك يطلق على "مصفاة الحزم الاستاتيكية" انها مصفاة "غير ذكية" لأنها لا توفر الا القليل من الحماية ضد الأنواع المتقدمة من الهجوم، اذ انها لا تأخذ في الاعتبار سوى كمية محدودة من المعلومات و تكتفى بها لاتخاذ القرار بتمرير الحزمة او منعها. ويتم تنفيذ التصفية الاستاتيكية عادة عن طريق الموجهات.

وعلامات هذا الحقل عندما تنشط تكون على النحو التالي:

(SYN) تستخدم هذه العلامة لبدء جلسة الاتصال، وبعد إرسالها لا يجب أن تنشط في أي وقت آخر خلال جلسة الاتصال.

(FIN) تشير هذه العلامة إلى أن النظام المرسل يود إنهاء جلسة الاتصال الحالية.

(ACK) تشير هذه العلامة إلى أن هذه الرسالة عبارة عن رد على طلب معلومات سبق إرساله إلى الخادم الذي يرسل الرد المحتوي على هذه العلامة النشطة.

(RST) تعيد هذه العلامة حالة جلسة الاتصال الحالية إلى الوضع الأصلي (Reset)، ويتم ذلك عادة في حالة حدوث فشل في عملية النقل لم يمكن التغلب عليه.

(URG) هذه العلامة تدل على احتواء الحزمة على معلومات ذات أولوية عالية (Urgent) مطلوب تمريرها على الفور، وعلى النظام المستقبل معالجة هذه الحزمة قبل أي بيانات أخرى قد تكون في الانتظار.

(PSH) مهمة هذه العلامة في حالة تنشيطها منع النظام المرسل من وضع البيانات في قائمة انتظار قبل إرسالها؛ فمعظم النظم المرسلة تضع البيانات في قوائم وذلك انتظارًا لمزيد من البيانات، وذلك بهدف تقليل عدد حزم الرسائل المرسلة.

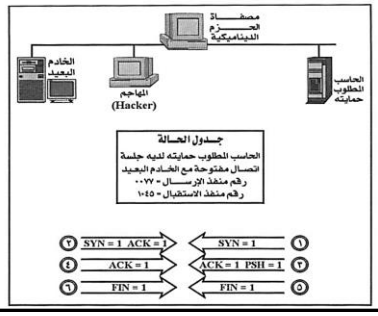
العلامات (TCP flags)

العلامة	الاسم	المعنى
SYN	مزامنة - (Synchronization)	تستخدم لإنشاء ارتباط (TCP)
ACK	اقرار - (Acknowledgment)	تُستخدم للإقرار باستلام البيانات أو حزم المزامنة
PSH	دفع - (Push)	إرشاد مكدس الشبكة بتجاوز التخزين المؤقت.
URG	عاجل - (Urgent)	يشير إلى حزم بيانات يجب معالجتها فوريا من قبل الشبكة قبل البيانات العادية.
FIN	نهاية - (Finish)	انهاء ارتباط (TCP) بأمان.
RST	إعادة ضبط - (Reset)	إنهاء الارتباط فورا وإسقاط أي بيانات أثناء النقل.

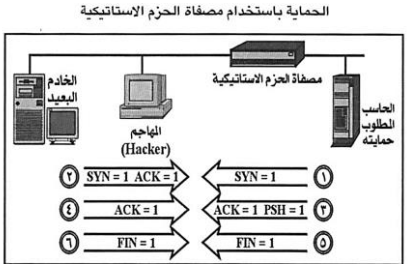
مصفاة الحزم : مصفاة الحزم الديناميكية

تتفوق "مصفاة الحزم الديناميكية" عن المصفاة الاستاتيكية باحتفاظها "بجدول الحالة" (State table) يمكنها من مراقبة حالة جلسة الاتصال، فهي لا تعتمد على محتويات حقل العلامات (TCP flags) وحده. ولتوضيح أهمية هذا الفارق نفترض ان احد المهاجمين ارسل حزمة بيانات للنظام في محاولة للتسبب في حدوث انهيار للنظام. هذا المهاجم يمكن ان يقوم بحيلة لخداع المصفاة، وذلك بان يجعل علامة (ACK) في حقل العلامات في وضع النشط (ACK=1) لكي يجعل الرسالة تبدو وكأنها استجابة لطلب احد المستفيدين بالشبكة المحلية. المصفاة الاستاتيكية يمكن ان تنخدع بهذه الحيلة و لكن المصفاة الديناميكية عند استقبال هذه الحزمة تقوم بمراجعة جدول الاتصال او "جدول الحالة"، عندئذ ستكتشف المصفاة انه لم يحدث أي اتصال مسبق مع هذا الموقع الذى وردت منه الرسالة.

الحماية باستخدام مصفاة الحزم الديناميكية



الحماية باستخدام مصفاة الحزم الاستاتيكية



يوضح الشكلان التاليان الفرق بين الحماية باستخدام مصفاة الحزم الاستاتيكية و المصفاة الديناميكية.

مصفاة الحزم : مصفاة الحزم الديناميكية

في الحالتين تحتوى قائمة التحكم في الاستخدام (ACL) و المخزنة في أي من المصفاتين على القواعد التالية:

1) السماح للحاسب المطلوب حمايته بإقامة أي جلسة اتصال مع الخادم البعيد للاستفادة من الخدمات التي يقدمها.
2) السماح بمرور الحزم التابعة لأى جلسة اتصال سبق اقامتها.
3) منع أي رسائل أخرى لا تحقق الشرطين السابقين.

وفقا للقاعدة الأولى يتم السماح للحاسب المطلوب حمايته ببدء جلسة اتصال مع الخادم البعيد. ويعني ذلك ان الحزمة التي تحتوى على علامة (SYN) نشطة (SYN=1) والتي تعنى بدء جلسة الاتصال يسمح لها بالمرور اذا كان مصدرها هو الحاسب المطلوب حمايته واذا كانت جهة الوصول هي الخادم البعيد، وذلك للسماح بكل أنواع الاستخدام للخدمات المتاحة على ذلك الخادم البعيد.

ووفقا للقاعدة الثانية يتم السماح بمرور كافة الحزم التي لا توجد بها علامة (SYN) نشطة (SYN=0)، مما يدل على انها رسائل تابعة لجلسة اتصال سبق اقامتها.

والقاعدة الثالثة تعني ان أي اتصال لا ينتمى بوضوح لإحدى القاعدتين السابقتين يجب منعه.

يستخدم كل من جداري الحماية في الشكلين السابقين نفس القواعد، ولكن يكون الاختلاف فيما لدى كل منهما من معلومات إضافية يبنى على أساسها قراره بالمرور. ويتضح من الشكلين ان الحاسوب المطلوب حمايته يبدأ جلسة اتصال مع الخادم البعيد (SYN=1) ويتم التعارف (SYN=1,ACK=1)، ثم يطلب الحاسب بعض البيانات من الخادم البعيد (ACK=1,PSH=1)، والذى يرد بالبيانات المطلوبة (ACK=1)، ثم يتم انها جلسة الاتصال بطلب من الحاسب (FIN=1) وموافقة الخادم البعيد (FIN=1).

مصفاة الحزم : مصفاة الحزم الديناميكية

المصفاة الاستاتيكية في الشكلين السابقين لا تنظر الا الى حقل العلامات (Flags) للتحقق من عدم وجود علامة (SYN) نشيطة (SYN=1) دليلا على ان هذه الحزمة جزء من جلسة اتصال قائمة بالفعل، ومن ثم تسمح لها بالمرور . اما المصفاة الديناميكية (في الشكلين السابقين) فهي تفعل الشيء نفسه ولكن مع انشاء سجل في جدول الحالة (State table) عند بدء الجلسة، وفي كل مرة يحاول الخادم البعيد الاستجابة للحاسب المطلوب حمايته تقوم المصفاة الديناميكية بمراجعة "جدول الحالة" للتأكد من ان الحاسب قد ارسل بالفعل في طلب بيانات من الخادم، وكذلك للتأكد من رقم منفذ الارسال ورقم منفذ الاستقبال في جدول الحالة، وانهما يطابقان الأرقام الواردة في حزمة البيانات المارة. كما تراجع المصفاة الديناميكية رقم الحزمة المتسلسل و رقم التعارف، و لا تسمح بمرور الحزمة الا بعد تطابق كل هذه البيانات. و بمجرد ورود الحزمة التي تحمل علامة (FIN) في الحالة النشطة (FIN=1) لأنهاء الجلسة يتم حذف السجل الذى يحتويه "جدول الحالة" وهذا السجل يتم حذفه كذلك اذا انقضت مدة معينة دون رد من احد الطرفين (مما يعنى ان خطأ ما قد حدث).

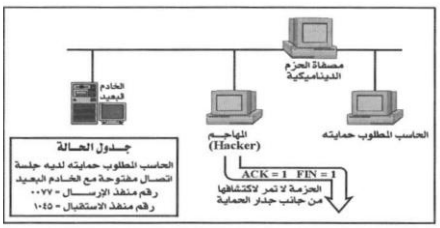
اذا حاول مهاجم خداع او مهاجمة الحاسب فعليه أولا ان يرسل اليه حزمة بها علامة (SYN) نشطة (SYN=1) لبدء جلسة اتصال مع الحاسب، وهذه الخدعة لن تجوز على المصفاتين (الاستاتيكية و الديناميكية) لان من المفروض ان هذه العلامة تكون هي وحدها النشطة في حقل العلامات اذا كانت اتية من الحاسب الداخلي (المطلوب حمايته) الى الخارج (الخادم) و ليس العكس.

وفى حالة ورودها من الخارج الى الداخل فلابد ان تكون مصحوبة بعلامة (ACK) نشطة اى (ACK=1)، لان الحاسبات في الشبكة الداخلية هي التي تطلب خدمات الموقع البعيد و ليس العكس. و ستتفطن كلا المصفاتين لهذه الخطأ و تحجب الرسالة. تحسبا لذلك سيقوم المهاجم بأرسال حزمة بها علامة (FIN) نشطة و علامة (ACK) نشطة (FIN=1,ACK=1).

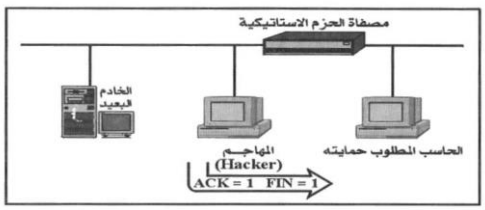
مصفاة الحزم : مصفاة الحزم الديناميكية

هذه الحزمة ستخدع المصفاة الاستاتيكية التي تأكدت فقط من عدم وجود علامة (SYN) نشطة وستسمح بمرور رسالة المهاجم. اما المصفاة الديناميكية فعند اكتشافها لعدم وجود علامة (SYN) نشطة ستقوم بمراجعة "جدول الحالة" وهنا ستكتشف عدم وجود جلسة اتصال قائمة مع المهاجم، ومن ثم تكتشف انه لا يوجد مبرر لمحاولة انهاء جلسة لم توجد أصلا، و ستكشف ان الجلسة المفتوحة هي مع الخادم البعيد و ليس مع المهاجم كما يوضح الشكلان التاليان.

جدار الحماية من نوع المصفاة الديناميكية لا ينخدع من جانب المهاجمين:



جدار الحماية من نوع المصفاة الاستاتيكية حيث تمر الحزمة التي تخدع المصفاة



مصفاة الحزم : مصفاة الحزم الديناميكية

والان ما لذى يجب على المهاجم فعله حتى يخدع جدار الحماية من نوع المصفاة الديناميكية؟، على المهاجم ان يقوم بما يلى:

- انتحال عنوان (IP) الخاص بالخادم البعيد.
- تحييد الخادم البعيد لضمان الا يرسل من جانبه أي استجابات للحاسب المطلوب اختراقه خلال الجلسة.
- إيجاد وسيلة لاستقبال الحزم المرسلة من الحاسب المطلوب اختراقه و قراءتها ليستطيع التصرف على هذه الأساس.
- معرفة منفذ الارسال ومنفذ الاستقبال المسجلين في "جدول الحالة".
- انتحال ارقام التسلسل (Sequence number) وأرقام التعارف (Acknowledgment number) للحزم المتبادلة.
- تنفيذ كل ما سبق بسرعة كبيرة تفاديا لتجاوز الفترة الزمنية المسموح بها (Timeout).

ويتضح من ذلك انه برغم ان هذه الخطوات السابقة ليست مستحيلة التنفيذ من جانب المهاجم، الا انها تجعل الأمور صعبة عليه، وهي تتطلب مهاجما خبيرا، كما تتطلب ان تكون الغنيمة باردة، أي تستحق العناء.

مما سبق يتضح ان جدران الحماية بمصفاة الحزم الديناميكية يمكن استخدامه لحماية الشبكة الداخلية، ولكن يعيب هذا النوع انه لا يبني احكامه على محتويات الحزمة ذاتها، انما يبنيها فقط على أساس ما تحتويه مقدمة الحزمة و جدول الحالة الذى يحتفظ به.

جدران الحماية : خادم البروكسي (Proxy)

جهاز الوكيل (Proxy) ويمكن ان يطلق عليه اسم "خادم البروكسي"، هو احد أنواع جدران الحماية القوية، وهو يتولى خدمات الانترنت من الشبكة نيابة عن المستفيد، مثل نقل الملفات (FTP)، او الدخول عن بعد (Telnet)، ومن ثم فهو يعمل كبوابة بين المستفيد و الانترنت. لذلك يطلق على هذا النوع من جدران الحماية اسم "بوابة التطبيقات" (Application-level gateway) او (Application gateway).

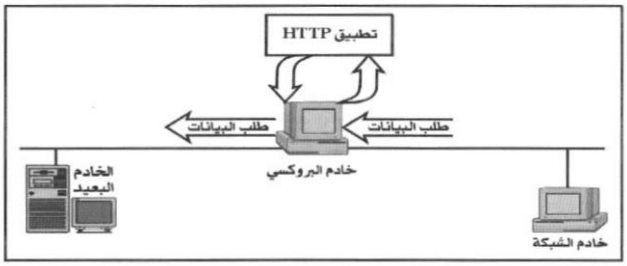
وهو قد يستخدم كجدار حماية بدلا من أسلوب تصفية حزم الرسائل، وباستخدام خادم البروكسي لا يتم الاتصال بين مرسل الرسالة و مستقبلها مباشرة ابدا و انما يلعب خادم البروكسي دور الوسيط بينهما.

على العكس من المصافي الديناميكية و الاستاتيكية فإن خادم البروكسي لا يقوم بتوجيه حزم الرسائل، لكنه يتفاهم مع كل طرف ممثلا للطرف الاخر، كأنه المترجم بين الطرفين.

يبين الشكل التالي قيام خادم البروكسي بدور الوسيط، حيث يرغب هنا حاسوب شبكة في طلب احدى صفحات الويب من خادم بعيد، فيقوم بصياغة الطلب و ارسال المعلومة المطلوبة الى خادم البروكسي الذى يعتبر البوابة المؤدية الى الشبكة البعيدة. بمجرد استلام خادم البروكسي لطلب البيانات فإنه يقوم بتحديد نوع الخدمة المطلوبة من جانب خادم الشبكة ويحدد التطبيق المستخدم و يمرر الطلب اليه.

جدران الحماية : خادم البروكسي (Proxy)

خادم البروكسي يقوم بدور الوسيط



جدران الحماية : خادم البروكسي (Proxy)

في المثال في الشكل كان المطلوب هو احدى صفحات الويب، ومن ثم تم توجيه الطلب الى تطبيق (HTTP) و هو عبارة عن برنامج يتم تنفيذه في ذاكرة خادم البروكسي، و مهمته الوحيدة هي التعامل مع (HTTP)، عند استلام (تطبيق-HTTP) لطلب البيانات يقوم بمراجعة "قائمة التحكم في الاستخدام" (ACL) للتأكد من السماح لهذا النوع من الرسائل بالمرور، وعند التأكد من ذلك يقوم خادم البروكسي بصياغة طلب جديد يقوم بإرساله الى الخادم البعيد وكأن هذا الطلب مرسل من خادم البروكسي و ليس من خادم الشبكة. ولذلك فعندما يقوم الخادم البعيد بالرد فإنه يرد على خادم البروكسي و الذى يقوم بدوره بتمرير الرد الى (تطبيق-HTTP) الذى يراجع البيانات الواردة، ثم يقوم خادم البروكسي بإنشاء حزمة رسائل جديدة ة يمررها الى خادم الشبكة. و يتضح ان طرفي الاتصال لا يتصلان ببعضهما مباشرة و انما يتم ذلك من خلال خادم البروكسي للتأكد من ان كل شيء على ما يرام.

يجد خادم البروكسي نفسه في وضع يسمح له بحجب بعض الرسائل في أي اتجاه، فيستطيع مثلا ان يتأكد من ان خادم الشبكة يستخدم كخادم للقراءة فقط من خارج الشبكة، وذلك عن طريق منه الرسائل القادمة من خارج الشبكة الى خادم البروكسي اذا كانت تحاول الكتابة او تعديل البيانات على خادم الشبكة.

جدار الحماية الشخصي

- يتحكم جدار الحماية الشخصي في حركة المرور بين حاسوب شخصي أو محطة عمل من جهة ، وشبكة الإنترنت أو شبكة المؤسسة على الجانب الآخر. يمكن استخدام وظيفة جدار الحماية الشخصي في بيئة المنزل وعلى إنترانت الشركة. عادةً ما يكون جدار الحماية الشخصي عبارة عن وحدة برمجية على الحاسوب الشخصي. في بيئة منزلية مع حواسيب متعددة متصلة بالإنترنت ، يمكن أيضًا وضع وظيفة جدار الحماية في جهاز توجيه يصل جميع ألحواسيب المنزلية بـجهاز (DSL) أو مودم كابل أو واجهة إنترنت أخرى. عادةً ما تكون جدران الحماية الشخصية أقل تعقيدًا بكثير من جدران الحماية المعتمدة على الخادم أو جدران الحماية المستقلة. يتمثل الدور الأساسي لجدار الحماية الشخصي في رفض الوصول غير المصرح به عن بُعد إلى الحاسوب. يمكن لجدار الحماية أيضًا مراقبة النشاط الصادر في محاولة لاكتشاف الفيروسات المتنقلة والبرامج الضارة الأخرى وحظرها.
- مثال على جدار الحماية الشخصي هو القدرة المضمنة في نظام التشغيل (Mac OS X). عندما يقوم المستخدم بتمكين جدار الحماية الشخصي في نظام التشغيل (Mac OS X)، يتم رفض جميع الاتصالات الواردة باستثناء تلك التي يسمح بها المستخدم صراحةً. لمزيد من الحماية ، قد تتوفر ميزات جدار الحماية المتقدمة ، مثل: وضع التخفي يخفي جهاز (Mac) على الإنترنت عن طريق إسقاط حزم الاتصال غير المرغوب فيها ، مما يجعله يبدو كما لو أنه لا يوجد جهاز (Mac). يمكن حظر حزم (UDP) ، مما يؤدي إلى تقييد حركة مرور الشبكة لحزم (TCP) على المنافذ المفتوحة فقط. قد يدعم جدار الحماية أيضًا تسجيل الاحداث ، وهو أداة مهمة للتحقق من النشاط غير المرغوب فيه.

مزايا مصافي حزم الرسائل:

يمتاز هذا النوع من جدران الحماية بعدة مزايا يمكن تلخيصها فيما يلي:

(١) يمكن حماية شبكة كاملة باستخدام موجه حاجب (Screening router) واحد عن طريق وضعه في المكان المناسب من الشبكة (عند التقاء الشبكة الداخلية بشبكة الإنترنت).

(٢) الكفاءة العالية للمصفاة البسيطة، فهنا تكمن الميزة في البساطة؛ لأن ذلك يعني تركيز الاهتمام في عدد محدود من مقدمات الحزم (Headers)، مما يعني عبئًا (Overhead) أقل على نظام التشغيل بعكس استخدام خادم البروكسي الذي يعني فحص محتويات الرسائل [Zwicky ٢٠٠٠].

(٣) الانتشار الواسع لهذا النوع وتعميم استخدامه في العديد من المنتجات يجعل من السهل العثور على الخبرات اللازمة لإدارته وتشغيله، والاطمئنان على إمكان وجوده في المواقع المختلفة وفي الدول المختلفة التي تقع بها فروع الشركة.

عيوب مصافي حزم الرسائل:

هناك بعض العيوب لهذا النوع من جدران الحماية نوجزها فيما يلي:

(١) أدوات التصفية المتوفرة حاليًا ليست على درجة عالية من الكفاءة؛ فالقواعد الموضوعة للرسائل المطلوب مراقبتها من الصعب تطبيقها، ومن الصعب اختبارها للتأكد من عملها بكفاءة، وقدرات هذا النوع من جدران الحماية تعتبر غير كاملة فهي لا تمنع كل أنواع الاقتحام، والأهم من ذلك وجود عيوب (Bugs) في العديد من البرمجيات المستخدمة في هذا النوع. في حالة وجود عيب في خادم البروكسي فإنه ببساطة يتوقف عن العمل بينما تستمر مصفاة الحزم في العمل في حالة وجود العيب مما يعني ثغرة أمنية خطيرة.

(٢) تحد مصفاة الحزم من كفاءة الموجه (Router)، فعملية التصفية للحزم تلقي بعبء إضافي على الموجه، خاصة إذا تعارضت القواعد المتبعة للتصفية مع بعض أساليب تحميل المعلومات في الذاكرة الخبيئة (Caching) فمثلاً في حالة استخدام وظيفة (Fast-path) في أجهزة شركة " سيسكو " (Cisco) يتم تنفيذ وظائف التوجيه الأساسية بالكامل من خلال بطاقة الشبكة (Network card)دون تدخل المعالج (CPU)، ولكن تنفيذ بعض قواعد التصفية يتطلب تدخل المعالج لفحص كل حزمة مما يسبب بطئًا في الأداء.

(٣) لا يمكن بسهولة فرض سياسات معينة مع بعض الموجهات التي تنفذ أسلوب تصفية الحزم، فهذه الموجهات لا تحتفظ بالمعلومات المطلوب استخدامها لتنفيذ السياسة الأمنية. فمقدمة الحزمة مثلاً تبين بوضوح الجهة المرسلة (Host) ولكنها لا تبين شخصية المرسل من داخل هذه الجهة، ومن ثم لا يمكن وضع أي نوع من القيود على الرسائل الصادرة من مستخدم معين، والأمر نفسه عند تحديد منفذ الاستقبال فيتم تحديد جهة الوصول وليس الشخص المفروض أن تصل إليه الرسالة. ويفتح هذا العيب الباب واسعًا أمام المقتحمين من الداخل للعبث بالرسائل. ولذلك تفرض بعض مصافي الحزم على المستخدم تعريف نفسه بدقة قبل إرسال الحزم، ومن ثم يمكن تصفية هذه الحزم وفقًا لاسم المستخدم. وإن كان ذلك يستبعد ميزة الشفافية التي كانت تحسب لهذا النوع من جدران الحماية.

مزايا استخدام خادم البروكسي:

لاستخدام خادم البروكسي (Proxy server) كجدار حماية عدة مزايا من بينها:

(١) يستخدم هذا النوع بشكل جيد في تسجيل وقائع الاستخدام (Logging)، ذلك لأن خادم البروكسي يستطيع فهم بروتوكولات التطبيق. فمثلاً بدلاً من تسجيل جميع حزم الرسائل المارة، فإن خادم البروكسي المتخصص في نقل الملفات (Proxy server FTP) يقوم فقط بتسجيل الأوامر المتبادلة بين الشبكة والخادم البعيد مما يؤدي إلى ترشيد استخدام سجل الوقائع وتوفير الوقت.

(٢) يقدم خادم البروكسي إمكانية استخدام الذاكرة الخبيئة (Caching) بالاحتفاظ بنسخة من طلبات البيانات، وذلك لأن جميع هذه الطلبات تمر عن طريق خادم البروكسي، وبالتالي إذا تكررت هذه الطلبات بشكل ملحوظ فإن الأداء يتحسن بشكل كبير.

(٣) يقوم خادم البروكسي بالتصفية بشكل أكثر كفاءة وأكثر ذكاء لأنه يفحص المحتوى، فهو أكثر قدرة على تصفية حزم (HTTP) على أساس نوع المحتوى، فيقوم مثلاً بمنع بعض برامج " جافا " أو " جافا سكريبت "، كما أنه أكثر قدرة من مصافي الحزم على كشف الفيروسات.

(٤) يستطيع هذا النوع من جدران الحماية تحديد شخصية المستخدم لأنه يتدخل في كل العمليات المارة به، ومن ثم يستطيع اتخاذ الإجراءات التي تتوقف على شخصية المستخدم. وهذه العملية تتم في حالة خادم البروكسي بشكل أكثر سهولة من مصافي الحزم.

(٥) يعالج هذا النوع حالات الخطأ في توليد الحزم من نوع (IP)، لأنه يكون موجودًا في موقع متوسط بين العميل وبين شبكة الإنترنت، ومن ثم فهو يقوم بتوليد حزم (IP) جديدة تحل محل تلك التي قام العميل بتوليدها، وبذلك يعالج أي خطأ قد يحدث من جانب العميل عند توليد هذه الحزم ولا ينخدع بها.

عيوب استخدام خادم البروكسي:

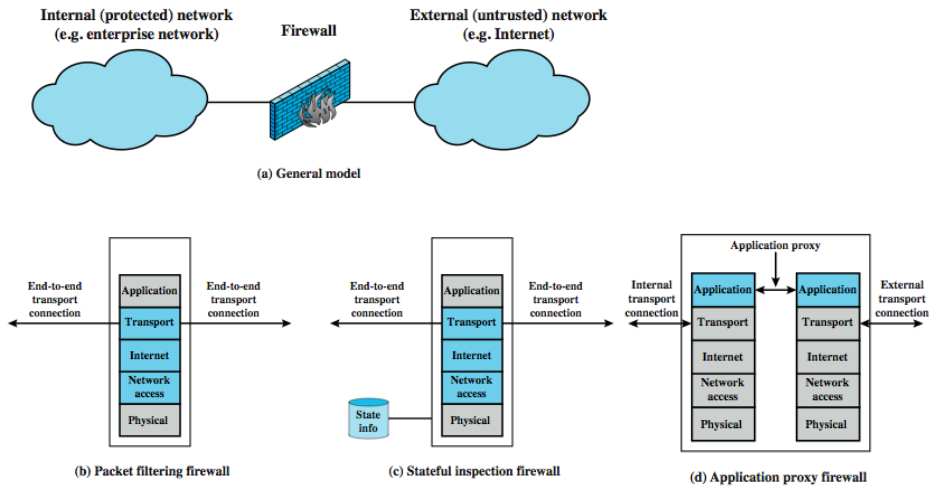
لا يمنع تعدد مزايا خادم البروكسي من وجود العديد من العيوب فيه، ومن هذه العيوب:

(١) تأتي معالجة الخدمات من جانب خادم البروكسي متأخرة عن ظهور هذه الخدمات التي تقدم على شبكة الإنترنت؛ فلابد من مرور فترة بين ظهور خدمة جديدة ومعالجة خادم البروكسي لها، فخادم البروكسي يعالج الخدمات القديمة المعروفة مثل خدمات نقل الملفات (FTP) والدخول عن بعد (Telnet)، أما ظهور خدمة جديدة فيحتاج إلى وقت حتى تتم إعادة برمجة خادم البروكسي ليستطيع التعامل مع هذه الخدمة، ويعتمد طول هذا الوقت أو قصره أساسًا على تصميم هذه الخدمة ومدى مناسبتها للمعالجة من جانب خادم البروكسي، الأمر الذي يجعل الاستخدام الآمن للخدمات الجديدة غير ممكن بشكل فوري من جانب المواقع المختلفة، إلى أن تتوفر خدمة البروكسي المقابلة. ووجه الخطورة هنا يكمن في أن الشركة التي تريد استخدام هذه الخدمة ستضطر لوضعها خارج نطاق خادم البروكسي حتى تستطيع الاستفادة منها، مما يشكل ثغرة أمنية. وقد ظهرت مؤخرًا خدمة خاصة تسمى (Generic proxy) تعالج هذا الأمر بعض الشيء.

(٢) قد يحتاج خادم البروكسي خادمًا خاصًا لكل خدمة من الخدمات (لكل بروتوكول)، وذلك لأن خادم البروكسي قد يحتاج إلى فهم البروتوكول حتى يتمكن من اتخاذ القرار المناسب بتمرير الحزمة أو حجبها، ومن أجل أن يستطيع التنكر في صورة العميل في مواجهة الخادم البعيد ويتنكر في صورة الخادم البعيد في مواجهة العميل (الحاسب المطلوب حمايته). ويشكل تعدد الخوادم وتهيئتها وإدارتها عبئًا غير يسير، إلا في حالة استخدام خدمة (Generic proxy) التي ذكرناها في الفقرة السابقة، ولكننا في هذه الحالة نكون أقرب إلى مصافي الحزم منا إلى خوادم البروكسي!

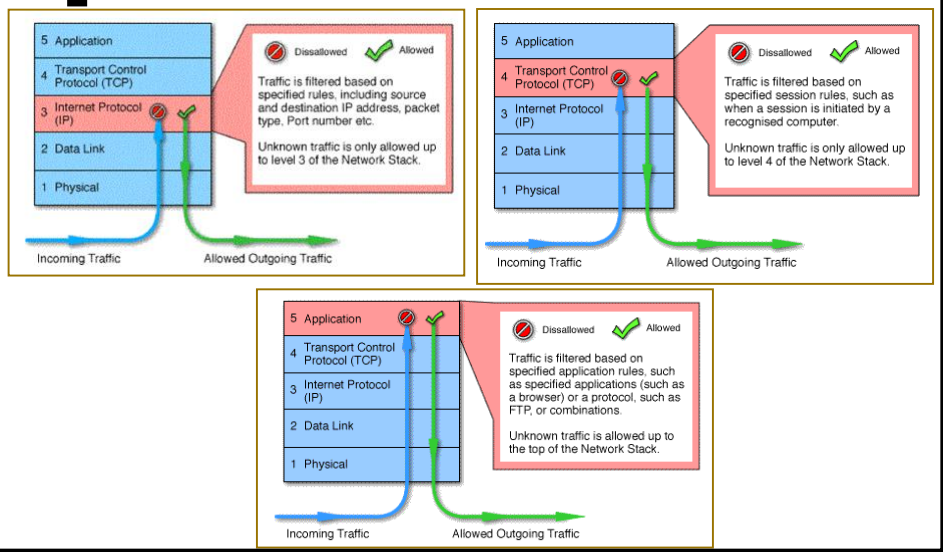
(٣) في كثير من الأحيان يتطلب استخدام خادم البروكسي إدخال تعديلات على أداء المستفيد وعلى عمل التطبيقات وعلى الإجراءات المتبعة، باستثناء تلك الخدمات المصممة أصلاً للاستخدام مع خادم البروكسي. وربما تسبب هذه التعديلات عيوبًا أخرى، أو تشكل عبئًا على المستخدم وعلى كفاءة تشغيل النظام.

أنواع جدران الحماية



مصفاة الحزم مقابل البوابة مقابل البروكسي

Packet Filtering vs Gateway vs Application-Level Firewall

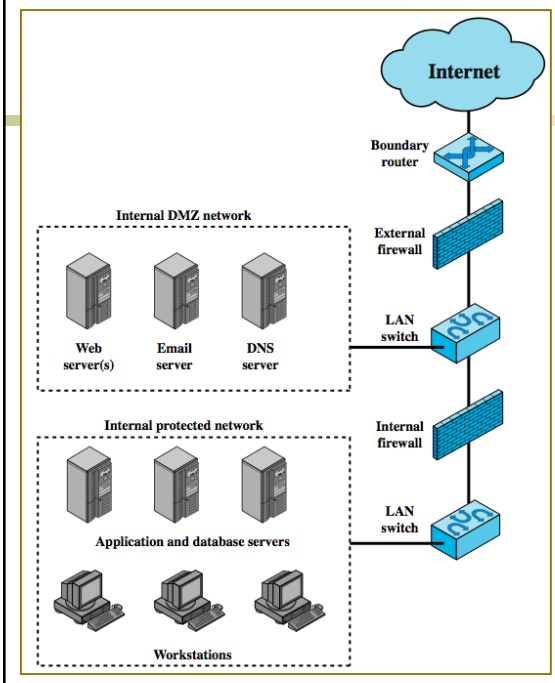


مواقع جدار الحماية

يتم وضع جدار الحماية لتوفير حاجز وقائي بين مصدر خارجي ، يحتمل أن يكون غير موثوق به لحركة المرور والشبكة الداخلية. مع وضع هذا المبدأ العام في الاعتبار ، يجب على مسؤول الأمان تحديد الموقع وعدد جدران الحماية المطلوبة.

- يقترح الشكل التمييز الأكثر شيوعًا ، وهو التمييز بين جدار الحماية الداخلي والخارجي. يتم وضع جدار حماية خارجي على حافة شبكة محلية أو شبكة مؤسسة. يعمل جدار حماية داخلي واحد أو أكثر على حماية الجزء الأكبر من شبكة المؤسسة. بين هذين النوعين من جدران الحماية يوجد جهاز واحد أو أكثر متصل بالشبكة في منطقة يشار إليها باسم شبكة (DMZ) - المنطقة المنزوعة السلاح. عادةً ما توجد شبكات الأنظمة التي يمكنها التواصل خارجيًا ولكنها تحتاج إلى الحماية في منطقة (DMZ).
- يوفر جدار الحماية الخارجي مقياسًا للتحكم في الوصول والحماية لأنظمة (DMZ) بما يتوافق مع حاجتها للاتصال الخارجي. يوفر جدار الحماية الخارجي أيضًا مستوى أساسيًا من الحماية لبقية شبكة المؤسسة.
- في هذا النوع من التكوين ، خادم جدران الحماية الداخلية ثلاثة أغراض:
  - يضيف قدرة تصفية أكثر صرامة ، مقارنة بجدار الحماية الخارجي ، من أجل حماية خوادم المؤسسة ومحطات العمل من الهجمات الخارجية.
  - يوفر حماية ثنائية الاتجاه فيما يتعلق بالمنطقة المجردة من السلاح ، ويحمي ما تبقى من الشبكة من الهجمات التي يتم إطلاقها من المنطقة المجردة من السلاح ويحمي أنظمة DMZ من الهجوم من الشبكة الداخلية المحمية.
  - يمكن استخدام العديد من جدران الحماية الداخلية لحماية أجزاء من الشبكة الداخلية من بعضها البعض. يوضح الشكل 5 التكوين الذي يتم فيه حماية الخوادم الداخلية من محطات العمل الداخلية والعكس صحيح.

مواقع جدار الحماية

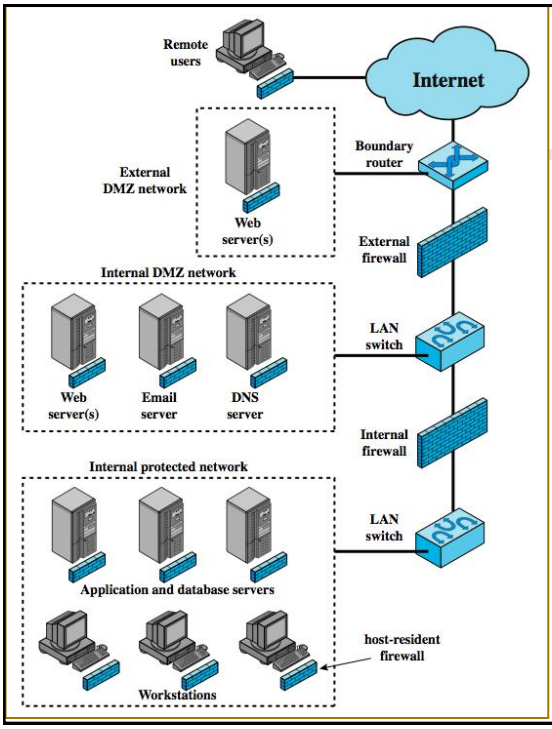


جدار الحماية الخارجي:
حماية للمنطقة منزوعة السلاح (DMZ) بما يتفق مع حاجتها للاتصال الخارجي

جدار الحماية الداخلي:
(أ) قدرة تصفية أكثر صرامة لتوفير الحماية من الهجمات الخارجية
(ب) يوفر حماية ثنائية الاتجاه لشبكة DMZ

جدران الحماية الموزعة

- يتضمن تكوين جدار الحماية الموزع أجهزة جدار حماية مستقلة بالإضافة إلى جدران الحماية المستندة إلى المضيف والتي تعمل معًا تحت تحكم إداري مركزي. يوضح الشكل تكوين جدار حماية موزع. يمكن للمسؤولين تكوين جدران الحماية الخاصة بالمضيف على مئات الخوادم ومحطات العمل بالإضافة إلى تكوين جدران الحماية الشخصية على أنظمة المستخدم المحلية والبعيدة. تتيح الأدوات لمسؤول الشبكة تعيين السياسات ومراقبة الأمان عبر الشبكة بالكامل. تعمل جدران الحماية هذه على الحماية من الهجمات الداخلية وتوفر الحماية المصممة لأجهزة وتطبيقات معينة. توفر جدران الحماية المستقلة حماية عالمية ، بما في ذلك جدران الحماية الداخلية وجدار الحماية الخارجي ، كما تمت مناقشته سابقًا.
- مع جدران الحماية الموزعة ، قد يكون من المنطقي إنشاء منطقتي (DMZ) داخلية وخارجية. يمكن وضع خوادم الويب التي تحتاج إلى حماية أقل نظرًا لوجود معلومات أقل أهمية عليها في منطقة (DMZ) الخارجية ، بعد جدار الحماية الخارجي. الحماية المطلوبة يتم توفيرها بواسطة جدران الحماية المعتمدة إلى المضيف في هذه الخوادم.
- من الجوانب المهمة لتكوين جدار الحماية الموزع مراقبة الأمان. تتضمن هذه المراقبة عادةً تجميع السجلات وتحليلها وإحصاءات جدار الحماية والمراقبة الدقيقة عن بُعد للمضيفين الفرديين إذا لزم الأمر.



جدران الحماية الموزعة

مزيج من جدران الحماية السابقة

جدار الحماية المقام علي عشرات من الحواسيب بالإضافة إلى جدران الحماية مستقلة تحت إدارة مركزية